"GFW"的前世今生，一部 GFW 之父方滨兴的发家史（2009）

标题的 GFW 之所以加上引号是因为，GFW 是局外人起的绰号，它的真实称呼并非如此，但"GFW"也确实如实涵盖了这一在中国一贯隐晦而模糊的概念。

时间表

- 1998 年 9 月 22 日，公安部部长办公会议通过研究，决定在全国公安机关开展全国公安工作信息化工程——"金盾工程"建设。

- 1999 年 4 月 20 日，公安部向国家计委送交金盾工程立项报告和金盾工程项目建议书。

- 1999 年 4 月 25 日，上万名法轮功练习者围攻中南海。

- 1999 年 6 月，国家计算机网络与信息安全管理中心成立，局级事业单位。

- 1999 年 7 月 22 日，中华人民共和国政府宣布法轮功妨碍国家安全和社会稳定，认定法轮大法研究会及法轮功为非法组织，决定予以取缔。

- 1999-2000 年，在哈尔滨工业大学任教多年的方滨兴调任国家计算机网络与信息安全管理中心副总工程师。

- 1999 年 12 月 23 日，国务院发文成立国家信息化工作领导小组，国务院副总理吴邦国任组长。其第一下属机构计算机网络与信息安全管理工作办公室设在已经成立的国家计算机网络与信息安全管理中心，取代计算机网络与信息安全管理部际协调小组，对"公安部、安全部、保密局、商用密码管理办公室以及信息产业部"等部门的网络安全管理进行组织协调。

- 2000-2002 年，方滨兴在国家计算机网络与信息安全管理中心任总工程师、副主任、教授级高级工程师。

- 2000 年 4 月 20 日，公安部成立金盾工程领导小组及办公室。

- 2000 年 5 月，005 工程开始实施。

- 2000 年 8 月 19 日，大纪元时报创刊。

- 2000 年 10 月，信息产业部组建计算机网络应急处理协调中心。

- 2000 年 12 月 28 日，第九届全国人民代表大会常务委员会第十九次会议通过《关于维护互联网安全的决定》。

- 2001 年，方滨兴"计算机病毒及其预防技术"获国防科学技术三等奖，排名第一。

- 2001 年，方滨兴获国务院政府特殊津贴、信息产业部"在信息产业部重点工程中做出突出贡献特等奖先进个人"称号，中组部、中宣部、中央政法委、公安部、民政部、人事部等联合授予"先进个人"称号。

- 2001 年 1 月 19 日，国家计算机网络与信息安全管理中心上海分中心成立，位于上海市黄浦区中山南路 508 号 6 楼。国家计算机网络应急技术处理协调中心上海分中心是工业和信息化部直属的中央财政全额拨款事业单位。

- 2001 年 4 月 25 日，"金盾工程"经国务院批准立项。

- 2001 年 7 月，计算机网络与信息安全管理工作办公室批准哈尔滨工业大学建立国家计算机信息内容安全重点实验室，胡铭曾、方滨兴牵头。

- 2001 年 7 月 24 日，国家计算机网络与信息安全管理中心广州分中心成立，位于广州市越秀区建中路 2、4 号。

- 2001 年 8 月 8 日，国家计算机网络与信息安全管理中心组建国家计算机网络应急处理协调中心，缩写 CNCERT/CC。

- 2001 年 8 月 23 日，国家信息化领导小组重新组建，中央政治局常委、国务院总理朱镕基任组长。

- 2001 年 11 月 28 日，国家计算机网络与信息安全管理中心上海互联网交换中心成立。提供"互联网交换服务，互联网骨干网华东地区数据交换，数据流量监测与统计，网间通信质量监督，交换中心设备维护与运行，网间互联费用计算，网间互联争议协调"，位于上海市黄浦区中山南路 508 号。

- 2001 年 11 月 28 日，国家计算机网络与信息安全管理中心广州互联网交换中心成立，位于广州市越秀区建中路 204 号。

- 2001 年 12 月，在北京的国家计算机网络与信息安全管理中心综合楼开始兴建。

- 2001 年 12 月 17 日，国家计算机网络与信息安全管理中心湖北分中心成立。

- 2002 年，方滨兴任中国科学院计算技术研究所客座研究员、博士生导师、信息安全首席科学家。2002-2006 年，方滨兴在国家计算机网络与信息安全管理中心任主任、总工程师、教授级高级工程师，升迁后任其名誉主任。

- 2002 年 1 月 25 日，报道称："国家计算机网络与信息安全管理中心上海互联网交换中心日前开通并投入试运行，中国电信、中国网通、中国联通、中国吉通等 4 家国家级互联单位首批接入。中国移动互联网的接入正在进行之中，近期可望成为第五家接入单位。"

- 2002 年 2 月 1 日，国家计算机网络与信息安全管理中心新疆分中心成立。

- 2002 年 2 月 25 日，国家计算机网络与信息安全管理中心贵州分中心成立。

- 2002 年 3 月 20 日，多个国家计算机网络与信息安全管理中心省级分中心同时成立。

- 2002 年 9 月 3 日，Google.com 被封锁，主要手段为 DNS 劫持。

- 2002 年 9 月 12 日，Google.com 封锁解除，之后网页快照等功能被封锁，手段为 TCP 会话阻断。

- 2002 年 11 月，经费 6600 万的国家信息安全重大项目"大范围宽带网络动态阻断系统"（大范围宽带网络动态处置系统）项目获国防科学技术二等奖。云晓春排名第一，方滨兴排名第二。哈尔滨工业大学计算机网络与信息内容安全重点实验室李斌、清华大学计算机系网络技术研究所、清华大学网格计算研究部杨广文有参与。

- 2003-2007 年，方滨兴任信息产业部互联网应急处理协调办公室主任。

- 2003 年 1 月 31 日，经费 4.9 亿的国家信息安全重大项目"国家信息安全管理系统"（005 工程）获 2002 年度国家科技进步一等奖，方滨兴排名第一，胡铭曾排名第二，清华大学排名第三，哈尔滨工业大学排名第四，云晓春排名第四，北京大学排名第五，郑纬民排名第七，中国科学院计算技术研究所有参与。

- 2003 年 2 月，在北京的国家计算机网络与信息安全管理中心综合楼工程竣工。

- 2003 年 7 月，国家计算机网络应急处理协调中心更名为国家计算机网络应急技术处理协调中心。

- 2003 年 9 月 2 日，全国"金盾工程"会议在北京召开，"金盾工程"全面启动。

- 2004 年，国家信息安全重大项目"大规模网络特定信息获取系统"，经费 7000 万，获国家科技进步二等奖。

- 2005 年，方滨兴任国防科学技术大学兼职教授、特聘教授、博士生导师。

- 2005 年，方滨兴被遴选为中国工程院院士。

- 2005 年，"该系统"已经在北京、上海、广州、长沙建立了互相镜像的 4 套主系统，之间用万兆网互联。每套系统由 8CPU 的多节点集群构成，操作系统是红旗 Linux，数据库用的是 OracleRAC。2005 年国家计算机网络与信息安全管理中心（北京）就已经建立了一套 384*16 节点的集群用于网络内容过滤（005 工程）和短信过滤（016 工程）。该系统在广州、上海都有镜像，互相以十万兆网链接，可以协同工作，也可以独立接管工作。

- 2006 年 11 月 16 日，"金盾工程"一期在北京正式通过国家验收，其为"为中华人民共和国公安部设计，处理中国公安管理的业务，涉外饭店管理，出入境管理，治安管理等的工程"。

- 2007 年 4 月 6 日，国家计算机网络与信息安全管理中心上海分中心机房楼奠基，位于康桥镇杨高南路 5788 号，投资 9047 万元，"……是国家发改委批准实施的国家级重大项目，目前全国只有北京和上海建立了分中心，它是全国互联网信息海关，对保障国家信息安全担负着重要作用。"

- 2007 年 7 月 17 日，大量使用中国国内邮件服务商的用户与国外通信出现了退信、丢信等普遍现象。

- 2007 年 12 月，方滨兴任北京邮电大学校长。

- 2008 年 1 月 18 日，信息产业部决定免去方滨兴的国家计算机网络与信息安全管理中心名誉主任、信息产业部互联网应急处理协调办公室主任职务，"另有职用"。

- 2008 年 2 月 29 日，方滨兴当选第十一届全国人民代表大会安徽省代表。

- 2009 年 8 月 10 日，方滨兴在"第一届中国互联网治理与法律论坛"上大力鼓吹网络实名制。

机构关系

国家计算机网络与信息安全管理中心（安管中心）是原信产部现工信部的直属部门。

安管中心与国家信息化工作领导小组计算机网络与信息安全管理工作办公室与国家计算机网络应急技术处理协调中心（CNCERT/CC，互联网应急中心）是一个机构几块牌子的关系。比如方滨兴简历中"1999-2000 年在国家计算机网络应急技术处理协调中心任副总工"与"计算机网络应急处理协调中心"的成立时间两种

说法就有着微妙的矛盾。实际上几个机构的人员基本一致。安管中心下属互联网交换中心与国家互联网络交换中心是不同的机构。各安管中心省级分中心一般挂靠当地的通信管理局。

安管中心的主要科研力量来自"哈尔滨工业大学一定会兴盛"方滨兴当博导有一批学生的哈工大以及关系良好的中科院计算所，这两个机构是那三个国家信息安全重大项目的主要参与者，之后还在不断吸引人才并为安管中心输送人才和技术。在方滨兴空降北邮之后，往安管中心输血的成分中哈工大的逐渐减少，北邮的逐渐增多。

CNCERT/CC 的国内"合作伙伴"有中国互联网协会主办北京光芒在线网络科技有限公司承办的中国互联网用户反垃圾邮件中心，是个没有实权的空壳；国家反计算机入侵及防病毒研究中心、国家计算机病毒应急处理中心，是公安部、科技部麾下；违法和不良信息举报中心是国新办势力范围；国家计算机网络入侵防范中心是中科院研究生院的机构，同样直接支撑 CNCERT/CC。

CNCERT/CC 的应急支撑单位中民营企业最初领跑者是绿盟，后来绿盟因其台谍案被罢黜，启明星辰取而代之。而安管中心具有一些资质认证、准入审批的行政权力，这可能是民间安全企业趋之若骛的原因。不过，民营企业并未参与到国家信息安全的核心项目建设中，安管中心许多外围项目交给民企外企做，比如像隔离器之类的访问限制设备外包给启明星辰以作为辅助、备用，或者在与他们在网络安全监测上有所交流。

GFW 与金盾没有关系

敏锐的读者从时间表应该已经看出这样的感觉了。实际上，GFW 与金盾就是没有关系，两者泾渭分明，有很多区别。

公安系统搞网络监控的是公安部十一局。

GFW 是"国家信息关防工程"的一个子工程，直接上级是国家信息化工作领导小组和信息产业部是政治局亲自抓的国防工程。这个工程主要监测发现有害网站和信息，IP 地址定位，网上对抗信息的上报，跟踪有害短信息和及时进行封堵。江泽民，朱镕基，胡锦涛，李岚清，吴邦国等多次视察该工程。

"国家信息关防工程"包括"国家信息安全管理系统"工程代号为 005；还有国家信息安全 016 工程等等。

GFW 主要是舆情情报系统的工具，而金盾主要是公安系统的工具。GFW 的总支持者是负责宣传工作的李长春，和张春江、江绵恒。最初的主要需求来自政治局、政法委、安全部、610 办；而金盾的总支持者是公安系统的高层人士，主要需求来自公安部门。GFW 主外，作网络海关用；而金盾主内，作侦查取证用。GFW 建设时间短，花费少，成效好；而金盾建设时间长，花费巨大（GFW 的十倍以上），成效不显著。

GFW 依附于三个国家级国际出入口骨干网交换中心从 CRS GSR 流量分光镜像到自己的交换中心搞入侵检测，再扩散到一些放在 ISP 那里的路由封 IP，位置集中，设备数量少；而金盾则是公安内部信息网络，无处不在，数量巨大。GFW 的科研实力雄厚，国内研究信息安全的顶尖人才和实验室有不少在为其服务，比如哈工大信息安全重点实验室、中科院计算所、软件所、高能所、国防科大、总参三部、安全部 9 局、北邮、西电、上海交大、北方交大、北京电子科技学院、解放军信息工程学院、解放军装甲兵工程学院、信产部中电 30 所、总参 56 所等等；另外几乎所有 985 211 高校都参与此工程。一些公司商业机构也参与某些外围工程项目如 Websense、packeteer、BlueCoat、华为、北大方正、港湾、启明星辰、神州数码也提供了一些辅助设备。中搜、奇虎、北京大正、雅虎等等参与了搜索引擎安全管理系统。在某些省市级的网络

机房里，接入监控的部门就五花八门了，有安全、公安、纪检、部队，等等；部署的设备也是五花八门；正规军、杂牌军、洋外援各自为战。

而金盾的科研实力较弱，公安系统的公安部第三研究所信息网络安全研发中心、国家反计算机入侵与防病毒研究中心都缺乏科研力量和科研成果，2008 年 8 月成立信息网络安全公安部重点实验室想与哈工大的重点实验室抗衡，还特意邀请方滨兴来实验室学术委员会，不过这个实验室光是电子数据取证的研究方向就没什么前景，而且也没什么研究成果。GFW 之父方滨兴没有参与金盾工程，而工程院里在支持金盾工程的是沈昌祥；实际上那个公安部重点实验室的学术委员会名单很是有趣，沈昌祥自然排第一，方滨兴因为最近声名太显赫也不好意思不邀请他，方滨兴可能也有屈尊与公安系统打好关系的用意。

GFW 发展和状况

GFW 主要使用的硬件来自曙光和华为，没有思科、Juniper，软件大部为自主开发。原因很简单，对国家信息安全基础设施建设，方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也一直强调"信息安全应该以自主知识产权为主"。何况 GFW 属于保密的国防工程而且 GFW 没有闲钱去养洋老爷，肥水不流外人田。李国杰是工程院信息工程部主任、曙光公司董事长、中科院计算所所长，GFW 的大量服务器设备订单都给了曙光。方滨兴还将安管中心所需的大型机大订单给李国杰、国防科大卢锡城、总参 56 所陈左宁三位院士所在单位各一份。所以 GFW 为什么那么多曙光的设备，GFW 为什么那么多中科院计算所的科研力量，为什么方滨兴成为中科院计算所和国防科大都有显赫的兼职，为什么方滨兴从老家哈尔滨出来打拼短短 7 年时间就入选工程院卢浮宫？就是因为方滨兴头脑灵活，做事皆大欢喜。

网上有人讽刺 GFW 夜郎自大，事实上这是盲目乐观，无知者无畏。GFW 的技术是世界顶尖的，GFW 集中了哈工大、中科院、北邮货真价实的顶尖人才， 科研力量也是实打实地雄厚，什么动态 SSL、Freenet、VPN、SSH、TOR、GNUnet、JAP、I2P、Psiphon，什么 Feed Over Email 算什么葱。所有的翻墙方法，只要有人想得到，GFW 都有研究并且有反制措施的实验室方案储备。比如说：串接式封堵， 采用中间人攻击手段来替换加密通信双方所用的没有经过可信赖 CA 签名保护的数字证书网关/代理间的证书协调，在出口网关上进行解密检测也就是所谓深度内容检测，七层过滤。HTTPS 是需要认证的，客户端访问服务器时，服务器端提供 CA 证书，但有些实现也可以不提供 CA 证书。那么对于不提供 CA 证书的服务器，防火墙处理很简单，一律屏蔽掉。另外检测默认的 CA 发证机构，如果证书不是这些机构（Verisign、Thawte、Geotrust）发的，杀无赦。就是在客户端与服务器端进行 https 握手的阶段，过滤掉一切无 CA 证书或使用不合法 CA 证书的 https 请求。这一步是广谱过滤，与服务器的 IP 地址无关。

GFW 主要是入侵防御系统，检测-攻击两相模型。所有传输层明文的翻墙方案，检测然后立即进行攻击是很容易的事情；即使传输层用 TLS 之类的加密无法实时检测，那种方案面向最终用户肯定是透明的，谁也不能阻止 GFW 也作为最终用户来静态分析其网络层可检测特征。入侵检测然后 TCP 会话重置攻击算是干净利落的手段了，最不济也能通过人工的方式来查出翻墙方法的网络层特征（仅仅目标 IP 地址就已经足够）然后进行定点清除。如果是一两个国家的敌人，GFW 也能找到集群来算密钥。GFW 是难得能有中央财政喂奶的科研项目。那些在哈工大地下室、中科院破楼里的穷研究生即使没有钱也能搞出东西来，现在中央财政喂奶，更是干劲十足了。GFW 什么都行，就是 P2P 没办法，因为匿名性太好了，既不能实时检测出来，也无法通过静态分析找到固定的、或者变化而可跟踪的网络层特征。就这样也能建两个陷阱节点搞点小破坏，而且中科院的 242 项目"P2P 协议分析与测量"一直都没停。什么时候国外开学术会议还是 Defcon 谁谁发一篇讲 Tor 安全性的 paper，立即拿回来研究一番实现一下，已然紧跟学术技术最前沿了。不过实际

上，即使 GFW 这样一个中国最顶尖的技术项目也摆脱不了山寨的本性，就是做一个东西出来很容易，但是要把东西做细致就不行了。

不过可能有人就疑问，为什么 GFW 什么都能封但又不真的封呢？我的这个翻墙方法一直还是好好的嘛。其实 GFW 有它自己的运作方式。GFW 从性质上讲是纯粹的科研技术部门，对政治势力来说是一个完全没有主观能动性的工具。GFW 内部有很严格权限管理，技术与政治封装隔离得非常彻底。封什么还是解封什么，都是完全由上峰决定，党指挥枪，授权专门人员操作关键词列表，与技术实现者隔离得很彻底，互相都不知道在做什么。所以很多时候一些莫名其妙的封禁比如封 freebsd.org 封 freepascal.org（可能都联想到 freetibet.org），或者把跟轮子的 GPass 八杆子打不着的"package.debian.org/zh-cn/lenny/gpass"列为关键词，都是那些摆弄着 IE6 的官僚们的颐指气使，技术人员要是知道了都得气死。方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中讲一个立足国情的原则，说："主要是强调综合平衡安全成本与风险，如果风险不大就没有必要花太大的安全成本来做。在这里面需要强调一点就是确保重点的，如等级保护就是根据信息系统的重要性来定级，从而施加适当强度的保护。"所以对于小众的翻墙方式，GFW 按照它的职能发现了也就只能过一下目心里有个底，上峰根本都不知道有这么一种方式所以也根本不会去封、GFW 自己也没权限封，或者知道了也懒得再花钱花精力去布置。枪打出头鸟，什么时候都是这样。目前的状况是对于敏感数据能通过封锁基本上就是安全的，否则就被过滤掉了，对于庞大的网络数据用人来分析是不可能的，敏感数据只能基于过滤技术根据数据流里面的一些特征来发现，目前的解密技术对于庞大数据流量和加密技术想使用解密的方法是不可能实现的，只要加密数据流没有可识别的特征，过滤技术就不会有任何记录和反映，因此过滤技术是无法真正实现网络封锁的，因此必需加入新的参数，它们选择了量，即保存你的一段时间的数据。现在的破网方法用的比较多得是动态网，无界，花园，等等，由于接点相对来说是有限的和可知的，因此保存一段时间的数据就有了意义，由于使用破网软件的人很多，不可能人人都抓，可以根据量来区分出重点，和经常使用破网软件的人。当然你可以通过代理来连接这些可知接点来解决这个问题，破网软件也提供了这样的方法，但是通过代理联接可知的接点的请求还是可能被截获的。

方滨兴一个人把 GFW 崛起过程中的政治势能全部转化为他的动能之后就把 GFW 扔掉了。现在 GFW 是平稳期，完全是清水衙门，既没有什么后台，也无法再有什么政治、资金上的利益可以攫取，也无法再搞什么新的大型项目，连 IPv6 对 GFW 来说都成了一件麻烦事情。方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也感慨道："比如说 Web 2.0 概念出现后，甚至包括病毒等等这些问题就比较容易扩散，再比如说 IPv6 出来之后，入侵检测就没有意义了，因为协议都看不懂还检测什么……"GFW 一直就没有地位，一直就是一个没人管的萝莉，国新办、网监、广电、版权、通管局之类的怪蜀黍都压在上面要做这做那。所以方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中也首先强调一个机制，"需要宏观层面，包括主管部门予以支持。"所以，想解封网站，不要去找 GFW 本体，那没用，要去找 GFW 的上峰，随便哪个都行。而 ISP 就根本跟 GFW 没关系了，都不知道 GFW 具体搞些什么，起诉 ISP 完全属于没找到脉门。

不过 GFW 现在还是运行得很好，工作能力还有很大潜力可挖，唯一害怕的就是 DDoS 死撞墙。GFW 的规模在前面的时间表里也有数字可以估计，而且 GFW 现在的网站封禁列表也有几十万条之多。网络监控和对 MSN、YMSG、ICQ 等 IM 短信监控也都尽善尽美。GFW 在数据挖掘和协议分析上做的还比较成功，多媒体数据如音频、视频、图形图像的智能识别分析、自然语言语义判断识别、模式匹配、p2p、VoIP、IM、流媒体、加密内容识别过滤、串接式封堵等等是将来的重点。不过 GFW 也没有像机器学习之类的自组织反馈机制来自动生成关键词，因为它本身没有修改关键词的权限，所以这种技术也没必要，况且国内这种技术也是概念吹得多，论文发得多，实践不成熟。现在 GFW 和金盾最想要的就是能够从万草从中揪出一小撮毒草

的数据挖掘之类的人工智能技术。方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中提到"舆情驾驭核心能力"，"首先要能够发现和获取，然后要有分析和引导的能力"。怎么发现？就靠中科院在研的 973 课题"文本识别及信息过滤"和 863 重点项目"大规模网络安全事件监控"这种项目。 金盾工程花大钱搞出来，好评反而不如 GFW，十一局的干警们脸上无光无法跟老一辈交代啊。公安系统的技术力量跟 GFW 没法比，不过公安系统有的是钱，先游山玩水吃喝一通，然后把剩下的税金像冲厕所一样随便买个几十万个摄像头几万台刀片几十 PB 硬盘接到省市级网络中心，把什么东西都记录下来。问题是记下来不能用，只能靠公安干警一页一页地翻 Excel。所以说，虽然看起来 GFW 千疮百孔，金盾深不可测，只是因为公安部门比起 GFW 来比较有攻击性，看到毒草不是给你一个 RST 而是给你一张拘留证。反而是 GFW 大多数时候都把毒草给挡住了，而大多数毒草金盾都是没发现的。

国家信息安全话语范式

在轮子闹事被取缔之后，轮子组织仍然在从四面八方进行各种手段的宣传，而且逐渐依靠上了各种境外背景。境内的宣传活动很快就被公安和国安清理掉了，然而从境外网上而来的大量网络宣传让从未有过网络化经验的中央无所适从、毫无办法、十分着急。这些东西对中央来说都是难以忍受的安全威胁，因为这些威胁又发生在网上，自然国家网络安全就被提上了首要议程。适逢信息化大潮，电子政务概念兴起，中央下决心好好应对信息化的问题，于是就成立了国家信息化工作领导小组。我们可以看到，首批组成名单中，安全部门和宣传部门占了大多数席位，而且其第一下属机构就是处理安全问题，第二下属才是处理信息化改革，安全需求之强烈，可见一斑。正是这个时候，一贯对信息安全充满独到见解的方滨兴被信产部的张春江调入了安管中心练级。方滨兴对信息安全的见解与高层对网络安全的需求不谋而合。一个方滨兴见解的集大成概括，方滨兴在他最近的讲话《五个层面解读国家信息安全保障体系》中说："一定要有一个信息安全法，有了这个核心法你才能做一系列的工作。"国家信息安全体系的首要核心就是以信息安全为纲的法律保障体系，通过国家意志——法律来定义何谓"信息安全"。信息安全本来是纯技术、完全中性 的词语，通过国家意志的定义，将"煽动...煽动...煽动...煽动...捏造...宣扬...侮辱...损害...其他..."定义为所谓的网络攻击、网络垃圾、网络有害信息、网络安全威胁，却在实现层面完全技术性、中立性地看待安全，丝毫不考虑现实政治问题。这样既在技术上实现完备的封装，也给了用户以高可扩展性的安全事件定义界面。对国家安全与技术安全实现充满隐喻的捆绑，对意识形态与信息科学进行牢不可破的焊接，这就是方滨兴带给高层的开拓性思维，这就是方滨兴提出的国家信息安全话语范式。

这个话语范式是如此自然、封装得如此彻底，以至于几乎所有人都没有意识到中国的网络化发展出现了怎样严重的问题。几乎所有网民都没有意识到，给他们带来巨大麻烦和沮丧的 GFW 竟然是本来应该为网民打黑除恶的国家互联网应急响应中心；几乎所有网民都没有意识到，自己在网上某处的一亩三分地修剪花草对于国家来说竟然是网络安全攻击事件；几乎所有决策者都没有意识到，那个看似立竿见影的防火墙实际上具有怎样强大的副作用、会给互联网发展带来怎样大的伤害；几乎所有决策者都没有意识到，使用 GFW 这样专业的安全工具来进行网络封锁意味着什么。意识形态面对网络化这样变幻莫测的景色无法忍受，就只能用眼罩封闭住眼睛。在讨论网络化的中文理论文本中，摆到首要位置占据最多篇幅的便是网络安全和网络威胁。国家信息化工作领导小组第一下属机构便是处理安全问题。这样，在网络本身都没有发展起来的时候，就在理论上对网络进行种种限制和控制；在网络仍然自发地成长起来以后，便在文化上对网络进行系统性妖魔化，在地理上对网络中国进行闭关锁国。更严重的是，在根本不了解技术本质和副作用的情况下使用国家信息安全工具，就像一个不懂事的小孩把玩枪械。在维护安全的话语之下，决策者根本不知

道使用 GFW 进行网络封锁就是在自己的网络国土上使用军队进行镇压，切断网线就是在自己的网络国土上种蘑菇。

更悲哀的是，GFW 的建设者们大多都没有意识到他们在做的究竟是什么事情，在签订保密协议之后就无意识中投身党国事业滚滚长江东逝水。像云晓春这种跟着方滨兴出来打江山的，方滨兴倒是高飞了，云晓春们就只能鞠躬尽瘁干死技术，在安管中心反而被王秀军、黄澄清之辈后来居上。而当初在哈工大跟着方滨兴的穷研究生们，最后也陆陆续续去了百度之类的公司。GFW 面临与曼哈顿工程一样的伦理困局。科学本是中立的，但科学家却被政治摆弄。技术工作者们只关心也只被允许关心如何实现安全，并不能关心安全的定义到底如何。他们缺乏学术伦理精神，不能实践"对自己工作的一切可能后果进行检验和评估；一旦发现弊端或危险，应改变甚至中断自己的工作；如果不能独自做出抉择，应暂缓或中止相关研究，及时向社会报警"的准则。结果就算他们辛辛苦苦做研究却也不能造福民生，反而被扣上"扼杀中国人权""纳粹帮凶"的帽子，不可谓不是历史的悲哀。这种话语范式浸透了社会的方方面面。在这种话语之下，中国有了世界上最强大的防火墙，但中国的网络建设却远远落后于世界先进水平；中国有了世界上最庞大的网瘾治疗产业链，但中国的网络产业却只会山寨技；中国有了世界上最多的网民，但在互联网上却听不见中国的声音。GFW 已经实现了人们的自我审查，让人们即使重获自由也无法飞翔，完成了其根本目的。现在即使对 GFW 的 DDoS 的技术已经成熟，然而推倒墙却也变得没有意义，只能让公安系统的金盾得势，更多的网民被捕，最终新墙竖起。这一切都出自意识形态化现代性与网络化后现代性之间巨大断裂，以及"国家信息安全话语"这种致命的讳疾忌医。

结语

一部 GFW 简史同时也是中国网络化简史。网络化既是技术变革，也是文化变革。网络文化这种"有害成份"无法分而治之，因为网络化的技术变革与文化变革是一体的；后现代的网络文化也无法与现代的意识形态文化进行同化，因为两者分属不同的范式。网络的确是意识形态完全的敌人，因为网络多元化文化要求取消意识形态的中心地位；但意识形态不是网络的敌人，事实上网络没有敌人，因为网络只有解构对象。因此对于执政者来说，意识形态的中心地位与网络化发展趋势两者只能选择其一。实际情况是，执政者选择了前者，而把大刀挥向了 Web 2.0。于是网络用它一贯调侃的风格模仿意识形态话语进行了如下讽刺："我们对你陈旧的政权概念和意识形态烂腌菜毫不感兴趣。你无法理解在人类网络化的历史潮流之前宏大叙事为何而消解，你也无法理解国家和民族概念为何将分崩离析，你无法改变你对互联网的无知。你的政权无法成为我们真正的敌人。"其实，《2009 匿名网民宣言》只是过早的预言，cyberpunk 式的谜语。

然而，无论中国的互联网受到了怎样的限制和压迫，即便中国网民的眼界已经被成功禁锢，中国的网络还是以它自己的方式适应种种压力顽强地发展。无论有多么强大的 GFW 或者金盾，即使被关在果壳之中，网络仍然在以意识形态完全不能理解的方式走向后现代蓝海，自成为无限空间之王。

来自 <*http://web.archive.org/web/20170726195913/http://blog.renren.com/share/200487056/5148854419*>